APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,284	02/25/2004	Vincent J. Zimmer	42P18501	4006

7590 02/14/2007 R. Alan Burnett BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP Seventh Floor 12400 Wilshire Boulevard Los Angeles, CA 90025	EXAMINER JOHNSON, CARLTON

ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *22 November 2006*.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-20 and 23-28* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-20 & 23-28* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *2-25-2004* is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____.

        3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is responding to application papers filed **11-22-2006**.

2.   Claims **1 - 30** are pending.   Claims **1, 6, 11, 17, 20, 26** have been amended.

Claims **21, 22, 29, 30** have been canceled.   Claims **1, 11, 20, 26** are independent.

3.   *Response to Remarks*

3.1   **Applicant argues**, " ... *wherein the original portion of firmware comprises a*

startup portion of one of system management mode (SMM) firmware code and platform

management interrupt (PMI) firmware code ... ", is not disclosed by prior art. (see

Remarks Page 9, Lines 18-21); (Remarks Page 10, Lines 18-21)

The Chen and Gulick prior art combination discloses a startup portion of firmware

consisting of a system management mode (SMM) and a platform management interrupt

(PMI) capability. (see Gulick col. 5, lines 34-40; col. 6, lines 17-22: system

management mode (SMM); col. 6, lines 32-35; col. 8, lines 55-60: management

interrupt processing, platform management interrupt (PMI))

The claim limitation is disclosed by the referenced prior art

3.2   **Applicant argues**, " ... *claim for 103(c)* ... ". *(see Remarks Page 11, Lines 9-*

26);

This issue is moot based on new grounds of rejection.

3.3   The Examiner has considered the applicant's remarks concerning the execution of

platform firmware as a trusted process.

After an additional analysis of the applicant's invention, remarks, and a search of

the available prior art, it was determined that the current set of prior art consisting of

Chen (7,069,439), Challener (20050138393) and Gulick (7,065,654) discloses the

applicant's invention including disclosures in Remarks dated November 22, 2006.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims **1 - 4, 6 - 10** are rejected under 35 U.S.C. 103(a) as being unpatentable

over **Chen et al.** (US Patent No. **7,069,439**) in view of **Gulick et al.** (US Patent No.

7,065,654).

With Regards to Claim 1, Chen discloses a method comprising:

b)   securely storing the measurement of the trusted original portion of firmware; (see

Chen col. 7, lines 52-57: store integrity metric or measurement)

c)   measuring an unqualified current portion of firmware; (see Chen col. 8, lines 6-

16: obtain an integrity metric measurement for a platform or firmware; col. 9, lines

13-20: functional block or portion (i.e. unqualified portion) of BIOS or firmware

utilized for a measurement to be compared against original portion)

d) retrieving the measurement of the trusted original portion of firmware; (see Chen

   col. 9, lines 49-54: retrieve from storage integrity metric or measurement for

   trusted platform)

e) comparing the measurement of the trusted original portion of firmware to the

   measurement of the unqualified current portion of firmware; (see Chen col. 9,

   lines 49-54: comparison between two integrity metrics to determine match) and

f) if the measurements match, executing the current portion of firmware as a trusted

   process. (see Chen col. 9, lines 49-54; col. 13, lines 9-13: match successful,

   trusted process executed)

Chen discloses wherein measuring a trusted, (see Chen col. 3, lines 1-4; col. 4, lines

26-31: Trusted Computing Platform concept, prior art 6,988,250), original portion of

firmware. (see Chen col. 8, lines 6-9: obtain an integrity metric or measurement of

trust state for platform firmware; col. 9, lines 5-13: col. 9, lines 13-20: functional

block or portion (i.e. original) of BIOS or firmware utilized for a measurement to

become trusted portion)   Chen does not specifically disclose the usage of platform

management interrupt (PMI) firmware and system management mode (SMM)

firmware.

However, Gulick discloses:

a) wherein the original portion of firmware comprises a startup portion of at least

one of system management mode (SMM) firmware code or platform

management interrupt (PMI) firmware code; (see Gulick col. 5, lines 34-40; col. 6,

lines 17-22: system management mode; col. 6, lines 32-35; col. 8, lines 55-60:

management interrupt processing (i.e. platform management interrupt)

It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Gulick to enable the usage of platform management firmware and

system management firmware.   One of ordinary skill in the art would have been

motivated to employ the teachings of Gulick in order to enable the capability to

provide protection, security and ownership rights for user and corporate IT

environments.   (see Gulick col. 2, lines 11-16: " ... *From a hardware point of view,*

an x86 operating environment provides little for protecting user privacy, providing

security for corporate secrets and assets, or protecting the ownership rights of

content providers. All of these goals, privacy, security, and ownership (collectively,

PSO) are becoming critical in an age of Internet-connected computers. ... "; col. 2,

lines 19-20: " ... *From a software point of view, the x86 operating environment is*

equally poor for PSO. ... ")

With Regards to Claim 2, Chen discloses the method of claim 1, wherein securely

storing the measurement of the trusted portion of original firmware comprises storing

the measurement in a trusted platform module (TPM). (see Chen col. 7, lines 52-57; col.

9, lines 49-54; col. 9, lines 65-67: store an integrity metric or measurement within

trusted platform or firmware)

With Regards to Claims 3, 4, Chen discloses the method of claim 2, wherein the

trusted platform module is embodied as a hardware component or embodied as a

software-based component. (see Chen col. 7, lines 44-46: software or programmed

microcontroller, hardware implementation as an Integrated Circuit (IC))

With Regards to Claim 6, Chen discloses the method of claims 1, wherein

measuring the unqualified current portion of firmware comprises measuring a current

portion of at least firmware code. (see Chen col. 8, lines 6-9: measure integrity metric or

measurement of trusted state for platform firmware; col. 7, lines 19-21; col. 9, lines 43-

44: secure boot or startup procedure)   Chen does not specifically disclose the usage of

platform management interrupt (PMI) firmware and system management mode (SMM)

firmware.   However, Gulick discloses wherein at least one of system management

mode (SMM) firmware code or platform management interrupt (PMI) firmware code.

(see Gulick col. 5, lines 34-40; col. 6, lines 17-22: system management mode; col. 6,

lines 32-35; col. 8, lines 55-60: management interrupt processing (i.e. platform

management interrupt)

It would have been obvious to one of ordinary skill in the art to have modified Chen

as taught by Gulick to enable the usage of platform management firmware and system

management firmware.   One of ordinary skill in the art would have been motivated to

employ the teachings of Gulick in order to enable the capability to provide protection,

security and ownership rights for user and corporate IT environments.   (see Gulick col. 2, lines 11-16; col. 2, lines 19-20)

With Regards to Claim 7, Chen discloses the method, article of manufacture of claims 1, further comprising performing a core root of trust measurement (CRTM). (see Chen col. 8, lines 4-9: measure integrity metric or root of trust measurement)

With Regards to Claim 8, Chen discloses the method of claim 7, wherein the CRTM is a static CRTM comprising a measurement of a trusted bootable portion of firmware. (see Chen col. 7, lines 19-21: integrity metric or measurement acquired or utilized during trusted secure boot procedure)

With Regards to Claim 9, Chen discloses the method of claim 7, wherein the CRTM is a dynamic CRTM measured via execution of processor microcode. (see Chen col. 9, lines 10-20: microcode utilized to boot system, create a dynamic integrity metric or root of trust measurement based on portions of firmware generated from an ensemble digest)

With Regards to Claim 10, Chen discloses the method of claim 1, further comprising: creating a descriptor indicating where the trusted original portion of firmware is located. (see Chen col. 10, lines 16-21: certificate, containing or specify location of an integrity metric or measurement)

6.   Claims **5, 11 - 20, 23 - 28** are rejected under 35 U.S.C. 103(a) as being

unpatentable over **Chen-Gulick and further** in view of **Challener** (US PGPUB No.

20050138393).

With Regards to Claim 5, Chen discloses the method of claim 1, further comprising:

enforcing a security mechanism, wherein a processor must be operating to retrieve the

measurement of the trusted portion of firmware. (see Chen col. 3, lines 29-32:

processor; col. 3, line 67 - col. 4, line 1: security mechanism implemented; col. 8, lines

6-9: measure integrity metric or measurement)   Chen does not specifically disclose the

usage of access levels or locality within a trusted environment. However, Challener

discloses wherein enforcing a locality-based security mechanism, wherein a processor

must be operating in at least one of a given locality and a higher locality to retrieve the

measurement of the trusted portion of firmware. (see Challener paragraph [0015], lines

1-6; paragraph [0016], lines 9-12: access levels or locality utilized by trust

measurement)

It would have been obvious to one of ordinary skill in the art to have modified Chen

as taught by Challener to enable the capability to utilize access levels or locality. One

of ordinary skill in the art would have been motivated to employ the teachings of

Challener in order to leverage existing security systems. In addition, Challener enables

the implementation of a very secure multi-level security structure (i.e. unclassified,

classified, top secret), which enables access to information only by a user with a

security level equal to the level of the particular information. (see Challener paragraph

[0004], lines 1-13: " ... *allow users who have different levels of security to access a*

system ... implement a system in which stored data could be classified into two or more

levels of security and access to the data is controlled by the security level of the user ...

implemented system leveraged security mechanisms already found in some systems.

... ")

With Regards to Claim 11, Chen discloses a method, comprising: measuring at

least one integrity metric corresponding to a trusted portion of an original firmware

configuration. (see Chen col. 8, lines 6-9: measure an integrity metric or measurement

of trust state for platform firmware) Chen does not specifically disclose the usage of

platform management interrupt (PMI) firmware and system management mode (SMM)

firmware.

However, Gulick discloses:

a) wherein the original portion of firmware comprises a startup portion of at least

   one of system management mode (SMM) firmware code or platform

   management interrupt (PMI) firmware code; (see Gulick col. 5, lines 34-40; col. 6,

   lines 17-22: system management mode; col. 6, lines 32-35; col. 8, lines 55-60:

   management interrupt processing (i.e. platform management interrupt)

   It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Gulick to enable the usage of platform management firmware and

system management firmware.   One of ordinary skill in the art would have been

motivated to employ the teachings of Gulick in order to enable the capability to

provide protection, security and ownership rights for user and corporate IT

environments.   (see Gulick col. 2, lines 11-16; col. 2, lines 19-20)

Chen discloses storing a respective measurement corresponding to each of said at

least one integrity metric of a trusted platform module (TPM) and the secret

contained in a digest including the secret concatenated with the respective

measurement(s) (see Chen col. 7, lines 44-46: machine readable medium; col. 11,

lines 5-14: secret and integrity metric or measurement combined and stored within

digest), wherein a current firmware configuration includes a portion that matches the

trusted portion of the original firmware configuration. (see Chen col. 9, lines 49-54:

comparison between two integrity metrics to determine match)   Chen does not

specifically disclose storing a respective measurement corresponding to one

integrity metric in a corresponding platform configuration register (PCR) nor sealing

a secret to the TPM, the secret contained in a digest including the secret

concatenated with the respective measurement(s) stored in the PCR(s), wherein to

unseal the secret.

However, Challener discloses:

b) a respective measurement in a corresponding platform configuration register

    (PCR) of a trusted platform module(TPM); (see Challener paragraph [0019], lines

3-6; paragraph [0019], lines 11-12; paragraph [0020], lines 1-3: integrity metric or

measurement stored within a platform configuration register (PCR))

c) sealing a secret to the TPM, the secret, and to unseal the secret the integrity

metric or measurement combined with a secret. (see Challener paragraph

[0021], lines 1-8; paragraph [0031], lines 11-15: seal procedure utilized within a

trusted platform)

It would have been obvious to one of ordinary skill in the art to have modified Chen

as taught by Challener to enable the capability perform a seal procedure within a trusted

environment and to utilize platform configuration register (PCR). One of ordinary skill in

the art would have been motivated to employ the teachings of Challener in order to

leverage existing security systems. In addition, Challener enables the implementation

of a very secure multi-level security structure (i.e. unclassified, classified, top secret),

which enables access to information only by a user with a security level equal to the

level of the particular information. (see Challener paragraph [0004], lines 1-13)

With Regards to Claim 12, Chen discloses wherein concatenating the secret and

the respective measurement(s) used to form the digest. (see Chen col. 11, lines 5-14:

combine nonce or secret, and integrity metric or measurement stored within digest)

Chen does not specifically disclose specifying a locality to be associated with a trusted

firmware process nor concatenating the locality to the secret and the respective

measurement(s) used to form the digest stored in the PCR(s).

However, Challener discloses:

a) specifying a locality to be associated with a trusted firmware process and

concatenated with secret and measurement; (see Challener paragraph [0015],

lines 1-6; paragraph [0016], lines 9-12: access levels or locality utilized by trust

measurement, add access information to concatenation)

b) concatenating the locality to the secret and the respective measurement(s) used

to form the digest stored in the PCR(s). (see Challener paragraph [0015], lines 1-

6; paragraph [0016], lines 9-12: designate access levels or locality utilized by

trust measurement and combined in digest, add access information to

concatenation; paragraph [0019], lines 3-6; paragraph [0019], lines 11-12;

paragraph [0020], lines 1-3: integrity metric or measurement stored within a

platform configuration register (PCR))

It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Challener to enable the usage of access levels or locality, and

usage of platform configuration registers (PCRs).   One of ordinary skill in the art

would have been motivated to employ the teachings of Challener in order to

leverage existing security systems. In addition, Challener enables the

implementation of a very secure multi-level security structure (i.e. unclassified,

classified, top secret), which enables access to information only by a user with a

security level equal to the level of the particular information. (see Challener

paragraph [0004], lines 1-13)

With Regards to Claim 13, Chen and Challener combination discloses the method

of claim 11, further comprising:

a) asserting a locality corresponding to an execution privilege level; (see Challener

   paragraph [0015], lines 1-6; paragraph [0016], lines 9-12: access levels or

   locality utilized by trust measurement, locality or access, privileged level)

b) storing at least one of the respective measurement(s) in a PCR that may be

   extended if a current execution privilege level matches or exceeds the locality of

   the execution privilege level that is asserted; (see Challener paragraph [0019],

   lines 3-6; paragraph [0019], lines 11-12; paragraph [0020], lines 1-3: integrity

   metric or measurement stored within a platform configuration register (PCR);

   paragraph [0015], lines 1-6; paragraph [0016], lines 9-12: access levels or

   locality utilized by trust measurement, add access information to concatenation)

It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Challener to enable the usage of access levels or locality and

platform configuration register (PCRs) within a trusted environment. One of

ordinary skill in the art would have been motivated to employ the teachings of

Challener in order to leverage existing security systems. In addition, Challener

enables the implementation of a very secure multi-level security structure (i.e.

unclassified, classified, top secret), which enables access to information only by a

user with a security level equal to the level of the particular information. (see

Challener paragraph [0004], lines 1-13)

With Regards to Claim 14, Chen and Challener combination discloses the method

of claim 12, wherein the locality is locality 1. (see Challener paragraph [0015], lines 1-6;

paragraph [0016], lines 9-12: access levels or locality utilized by trust measurement)

It would have been obvious to one of ordinary skill in the art to have modified Chen

as taught by Challener to enable the usage of access levels or locality. One of ordinary

skill in the art would have been motivated to employ the teachings of Challener in order

to leverage existing security systems. In addition, Challener enables the

implementation of a very secure multi-level security structure (i.e. unclassified,

classified, top secret), which enables access to information only by a user with a

security level equal to the level of the particular information. (see Challener paragraph

[0004], lines 1-13)

With Regards to Claim 15, Chen discloses the method of claim 11, wherein the

trusted portion of the original firmware configuration includes a trusted boot block. (see

Chen col. 7, lines 19-21; col. 9, lines 43-44: secure boot, boot block utilized within

trusted device)

With Regards to Claim 16, Chen discloses the method of claim 15, further

comprising: measuring the trusted boot block to obtain a core root of trust measurement

(CRTM). (see Chen col. 8, lines 6-9: measure an integrity metric or root of trust

measurement; col. 7, lines 19-21: integrity metric or measurement for boot procedure

utilized)

With Regards to Claim 17, Chen discloses the method of claim 11 wherein

measuring the <u>current</u> portion of firmware comprises measuring a <u>current</u> portion of

firmware code. (see Chen col. 4, lines 60-64: trusted platform utilizing an integrity metric

or trust measurement; col. 7, lines 19-21: secure boot or startup procedure)   Chen does

not specifically disclose the usage of platform management interrupt firmware and

system management mode (SMM) firmware.   However, Gulick discloses wherein each

set of firmware components correspond to <u>at least</u> one of system management mode

(SMM) firmware code <u>or</u> platform management interrupt (PMI) firmware code. (see

Gulick col. 5, lines 34-40; col. 6, lines 17-22: system management mode; col. 6, lines

32-35; col. 8, lines 55-60: management interrupt processing (i.e. platform management

interrupt)

It would have been obvious to one of ordinary skill in the art to have modified Chen

as taught by Gulick to enable the usage of platform management interrupt firmware and

system management mode firmware.   One of ordinary skill in the art would have been

motivated to employ the teachings of Gulick in order to enable the capability to provide

protection, security and ownership rights for user and corporate IT environments.   (see

Gulick col. 2, lines 11-16; col. 2, lines 19-20)

With Regards to Claim 18, Chen discloses the method of claim 11, further

comprising wherein executing firmware as a trusted process. (see Chen col. 13, lines

9-13: execute trusted process)   Chen does not specifically disclose attempting to

unseal the secret sealed to the TPM nor executing firmware as a trusted process if the

secret is unsealed, otherwise executing the firmware process as an untrusted process.

However, Challener discloses:

a) attempting to unseal the secret sealed to the TPM; (see Challener paragraph

[0021], lines 1-8; paragraph [0031], lines 3-7: unseal procedure utilized within a

trusted platform) and

b) executing firmware as a trusted process if the secret is unsealed, otherwise

executing the firmware process as an untrusted process. (see Challener

paragraph [0021], lines 1-8; paragraph [0031], lines 3-7: unseal procedure

utilized within a trusted platform)

It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Challener to enable the capability to perform an unseal procedure

within a trust environment.   One of ordinary skill in the art would have been

motivated to employ the teachings of Challener in order to leverage existing security

systems. In addition, Challener enables the implementation of a very secure multi-

level security structure (i.e. unclassified, classified, top secret), which enables

access to information only by a user with a security level equal to the level of the

particular information. (see Challener paragraph [0004], lines 1-13)

With Regards to Claim 19, Chen discloses the method of claim 11, wherein the

integrity metric is measured by executing microcode on a processor. (see Chen col. 3,

lines 29-32: processor; col. 8, lines 6-9: measure integrity metric or measurement; col.

7, lines 46-47: execute programmable microcode on a trusted device)

With Regards to Claim 20, Chen discloses an article of manufacture, comprising:

a) a machine-readable medium have instructions stored thereon (see Chen col. 7,

lines 44-46: machine readable medium),

which when executed perform operations including:

b) measuring a trusted portion of an original set of firmware components during a

pre-boot phase of a computer system; (see Chen col. 8, lines 6-9: measure an

integrity metric or measurement of trust state for platform firmware)

d) measuring a portion of a current set of firmware components during an operating

system (OS)-runtime phase of the computer system determining if the

measurement of the portion of the current set of firmware components matches

the measurement of the portion of the original firmware components; (see Chen

col. 6, lines 34-42: BIOS or trusted device hands control over to OS) and

e) providing indicia to a processor to execute the portion of the current set of

firmware components as a trusted process if the measurements match. (see

Chen col. 13, lines 9-13: match successful, process executed)

Chen discloses wherein storing the measurement of the trusted portion of the

original set of firmware components. (see Chen col. 7, lines 52-57; col. 9, lines 49-

54: storage of integrity metric or measurement within certificate for trusted device)

Chen does not specifically disclose the usage of platform configuration register in trust operations.

However, Challener discloses:

c) storing the measurement of the trusted portion of the original set of firmware components in a trusted platform module (TPM) platform configuration register (PCR); (see Challener paragraph [0019], lines 3-6; paragraph [0019], lines 11-12; paragraph [0020], lines 1-3: integrity metric or measurement stored within a platform configuration register (PCR))

It would have been obvious to one of ordinary skill in the art to have modified Chen as taught by Challener to enable usage of platform configuration registers (PCRs) within a trust environment.   One of ordinary skill in the art would have been motivated to employ the teachings of Challener in order to leverage existing security systems. In addition, Challener enables the implementation of a very secure multi-level security structure (i.e. unclassified, classified, top secret), which enables access to information only by a user with a security level equal to the level of the particular information. (see Challener paragraph [0004], lines 1-13)

Chen does not specifically disclose the usage of platform management interrupt (PMI) firmware and system management mode (SMM) firmware.

However, Gulick discloses:

f) wherein the original portion of firmware comprises a startup portion of at least one of system management mode (SMM) firmware code or platform

management interrupt (PMI) firmware code; (see Gulick col. 5, lines 34-40; col. 6,

lines 17-22: system management mode; col. 6, lines 32-35; col. 8, lines 55-60:

management interrupt processing (i.e. platform management interrupt)

It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Gulick to enable the usage of platform management firmware and

system management firmware.   One of ordinary skill in the art would have been

motivated to employ the teachings of Gulick in order to enable the capability to

provide protection, security and ownership rights for user and corporate IT

environments.   (see Gulick col. 2, lines 11-16; col. 2, lines 19-20)

With Regards to Claim 23, Chen discloses the method, article of manufacture of

claim 20, further comprising performing a core root of trust measurement (CRTM). (see

Chen col. 8, lines 6-9: measure integrity metric or root of trust measurement)

With Regards to Claim 24, Chen discloses the article of manufacture of claim 20,

wherein the machine-readable medium (see Chen col. 7, lines 44-46: machine readable

medium; col. 11, lines 5-14: secret and measurement combined and stored within

digest) comprises further instructions to perform operations including: sealing a secret

to the TPM, the secret contained in a digest including the secret concatenated with the

measurement of the trusted portion of the original set of firmware that is stored in the

PCR. However, Challener discloses wherein to perform operations including: sealing a

secret to the TPM, the secret contained in a digest including the secret concatenated

with the measurement of the trusted portion of the original set of firmware that is stored

in the PCR. (see Challener paragraph [0021], lines 1-8; paragraph [0031], lines 11-15:

seal procedure utilized within a trusted platform; paragraph [0019], lines 3-6; paragraph

[0019], lines 11-12; paragraph [0020], lines 1-3: integrity metric or measurement stored

within a platform configuration register (PCR))

It would have been obvious to one of ordinary skill in the art to have modified Chen

as taught by Challener to seal a parameter within a trusted environment and utilize a

platform configuration register (PCR) for trust operations. One of ordinary skill in the

art would have been motivated to employ the teachings of Challener in order to

leverage existing security systems. In addition, Challener enables the implementation

of a very secure multi-level security structure (i.e. unclassified, classified, top secret),

which enables access to information only by a user with a security level equal to the

level of the particular information. (see Challener paragraph [0004], lines 1-13)

With Regards to Claim 25, Chen discloses the article of manufacture of claim 20,

wherein the article comprises a non-volatile memory device. (see Chen col. 7, lines 51-

52; col. 7, lines 19-21; col. 10, lines 16-21: non-volatile memory) Chen does not

specifically disclose a flash memory device. However, Challener discloses wherein the

article comprises a flash drive. (see Challener paragraph [0017], lines 7-11; paragraph

[0022], lines 1-6: flash memory)

It would have been obvious to one of ordinary skill in the art to have modified Chen

as taught by Challener to utilize a flash memory device. One of ordinary skill in the art

would have been motivated to employ the teachings of Challener in order to leverage

existing security systems. In addition, Challener enables the implementation of a very

secure multi-level security structure (i.e. unclassified, classified, top secret), which

enables access to information only by a user with a security level equal to the level of

the particular information. (see Challener paragraph [0004], lines 1-13)

With Regards to Claim 26, Chen discloses a system comprising:

a) a processor, including microcode instructions; (see Chen col. 7, lines 46-47:

microcontroller)

b) memory, operatively coupled to the processor; a trusted platform module,

operatively coupled to the processor; (see Chen col. 3, lines 29-32: processor;

col. 7, lines 39-42: memory) and

d) retrieving a first measurement stored in the TPM, the first measurement

comprising a measurement of a trusted portion of the firmware instructions; (see

Chen col. 7, lines 52-57; col. 9, lines 49-54: retrieve integrity metric or

measurement from certificate within trusted device)

f) comparing the first measurement to the second measurement; (see Chen col. 9,

lines 49-54: compare integrity metric or measurement values)

g) if the first and second measurements match, programming the microprocessor to

execute the current portion of firmware instructions as a secure process. (see

Chen col. 13, lines 9-13: execute process, if match successful)

Chen discloses a non-volatile or analogous flash type memory. (see Chen col. 7,

lines 51-52; col. 7, lines 19-21; col. 10, lines 16-21: flash or non-volatile memory)

Chen does not specifically disclose a flash type memory device.

However, Challener discloses:

c) a flash device having firmware instructions stored thereon (see Challener

   paragraph [0017], lines 7-11; paragraph [0022], lines 1-6: flash type memory

   utilized), which when executed on the processor perform operations including:

It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Challener to enable the usage of a flash type memory within a

trust environment. One of ordinary skill in the art would have been motivated to

employ the teachings of Challener in order to leverage existing security systems. In

addition, Challener enables the implementation of a very secure multi-level security

structure (i.e. unclassified, classified, top secret), which enables access to

information only by a user with a security level equal to the level of the particular

information. (see Challener paragraph [0004], lines 1-13)

Chen discloses wherein measuring a current portion of firmware instructions

analogous to the trusted portion of the firmware instructions to obtain a second

measurement. (see Chen col. 8, lines 6-9: obtain an integrity metric or

measurement of trust state for platform firmware) Chen does not specifically

disclose the usage of platform management interrupt (PMI) firmware and system

management mode (SMM) firmware.

However, Gulick discloses:

e) <u>wherein the original portion of firmware comprises a startup portion of at least</u>

   <u>one of system management mode (SMM) firmware code or platform</u>

   <u>management interrupt (PMI) firmware code</u>; (see Gulick col. 5, lines 34-40; col. 6,

   lines 17-22: system management mode; col. 6, lines 32-35; col. 8, lines 55-60:

   management interrupt processing (i.e. platform management interrupt)

   It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Gulick to enable the usage of platform management firmware and

system management firmware.   One of ordinary skill in the art would have been

motivated to employ the teachings of Gulick in order to enable the capability to

provide protection, security and ownership rights for user and corporate IT

environments.   (see Gulick col. 2, lines 11-16; col. 2, lines 19-20)

With Regards to Claim 27, Chen discloses the system of claim 26, wherein the

microcode instructions may be executed to perform the operations of generating a

dynamic core root of trust measurement (CRTM) for the system. (see Chen col. 8, lines

6-9: measure an integrity metric or measurement of trust state for platform firmware; col.

9, lines 10-20: microcode utilized to boot system creates a dynamic integrity metric or

root trust measurement based on portions of firmware generated from an ensemble

digest)

With Regards to Claim 28, Chen discloses the system of claim 26, wherein the

microcode instructions may be executed to perform operations including:

a) measuring the trusted portion of the firmware instructions to produce the first

measurement; (see Chen col. 8, lines 6-9: measure an integrity metric or

measurement of trust state for platform firmware, first measurement)

Chen discloses the storage of integrity metric or measurement. (see Chen col. 7,

lines 52-57; col. 9, lines 49-54: storage of integrity metric or measurement)   Chen

does not specifically disclose the usage of a platform configuration register (PCR).

However, Challener discloses:

b) storing the first measurement in a platform configuration register (PCR) of the

TPM. (see Challener paragraph [0019], lines 3-6; paragraph [0019], lines 11-12;

paragraph [0020], lines 1-3: integrity metric or measurement stored within a

platform configuration register (PCR); paragraph [0019], lines 16-20: integrity

metric or measurement stored within PCR)

It would have been obvious to one of ordinary skill in the art to have modified

Chen as taught by Challener to enable usage of platform configuration registers

(PCRs) within a trusted environment.   One of ordinary skill in the art would have

been motivated to employ the teachings of Challener in order to leverage existing

security systems. In addition, Challener enables the implementation of a very

secure multi-level security structure (i.e. unclassified, classified, top secret), which

enables access to information only by a user with a security level equal to the level

of the particular information. (see Challener paragraph [0004], lines 1-13)

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carlton Johnson whose telephone number is 571-270-

1032. The examiner can normally be reached Monday through Friday from 8:00AM to

5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nassar Moazzami, can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business.

Center (EBC) at 866-217-9197 (toll-free).

Carlton Johnson
February 9, 2007

NASSER M... ...
SUPERVIS... ... ...MINER
TECHN... 2100

2/12/07